PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-338868
(43)Date of publication of application : 08.12.2000

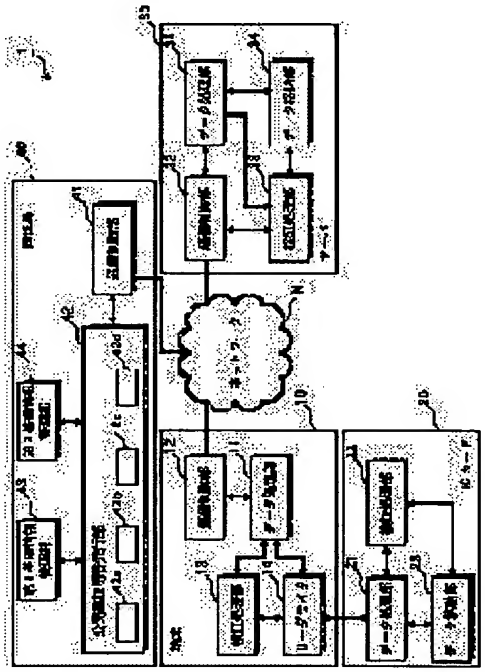
(51)Int.Cl. G09C 1/00
H04L 9/08
H04L 9/10
H04L 9/32

(21)Application number : 11-146311
(22)Date of filing : 26.05.1999

(71)Applicant : NTT DATA CORP
(72)Inventor : TAKAHASHI YOSHIO
TSUCHIYA SHIGEKI

(54) METHOD FOR ISSUING PUBLIC KEY CERTIFICATE, METHOD FOR VERIFYING, SYSTEM AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a system which can issue and verify a public key certificate capable of dealing with to a plurality of formats.
SOLUTION: A verification office 40 generates signature data for EMV use objecting fundamental information for the EMV use when receiving information applying an issue of a public key certificate. Also, it generates the signature data for X 509 use objecting information containing the fundamental information for the EMV use and the signature data for the EMV use. It issues the X 509 public key certificate containing all of the generated information and data. This X 509 public key certificate is converted into the EMV public key certificate at a terminal 10 in order to be able to use with an IC card 20.



LEGAL STATUS

[Date of request for examination] 08.11.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－338868
（P2000－338868A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.⁷		識別記号	FI		テーマコード*（参考）
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ　５Ｊ１０４
		６３０			６３０Ｆ
		６６０			６６０Ａ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｆ
	9/10				６２１Ａ

審査請求　未請求　請求項の数12　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平11－146311

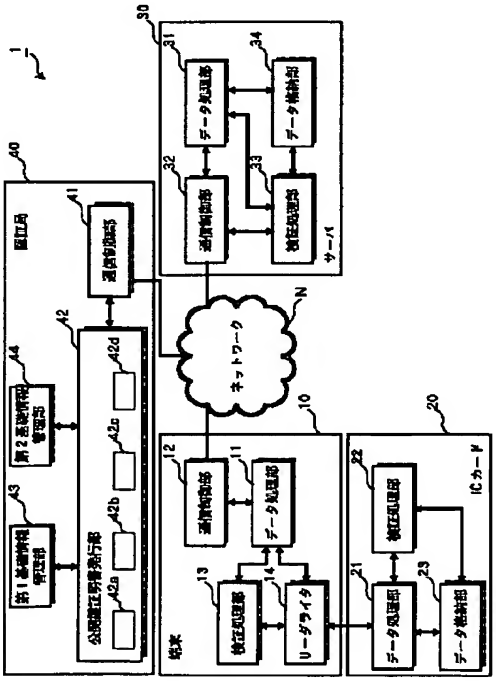
(22)出願日　平成11年５月26日(1999.5.26)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　高橋　芳夫
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　土屋　茂樹
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100099324
弁理士　鈴木　正剛

Ｆターム(参考)　5J104 AA09 AA16 EA05 JA21 LA03 LA06 MA02 NA12 NA35 PA07

(54)【発明の名称】　公開鍵証明書発行方法、検証方法、システム及び記録媒体

(57)【要約】
【課題】　複数のフォーマットに対応可能な公開鍵証明書を発行し、検証できるシステムを提供する。
【解決手段】　認証局４０は、公開鍵証明書の発行申請情報を受け取ると、ＥＭＶ用の基礎情報を対象としたＥＭＶ用の署名データを生成する。また、ＥＭＶ用の基礎情報とＥＭＶ用の署名データを含む情報を対象としたＸ５０９用の署名データを生成する。上記生成した情報及びデータをすべて含んだＸ５０９公開鍵証明書を発行する。このＸ５０９公開鍵証明書は、ＩＣカード２０で使用できるようにするため、端末１０でＥＭＶ公開鍵証明書に変換する。



1

【特許請求の範囲】

【請求項１】　所定の申請情報に基づいて生成された公開鍵証明書用の複数の基礎情報のうち、一のフォーマット用の基礎情報を対象とした当該一のフォーマット用の署名データを生成するとともに、

前記生成した基礎情報及び署名データと他のフォーマット用の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて前記他のフォーマット用の公開鍵証明書を作成する過程を含む、

公開鍵証明書の発行方法。

【請求項２】　請求項１記載の発行方法において作成された公開鍵証明書から前記一のフォーマット用の基礎情報、前記一のフォーマット用の署名データ、前記他のフォーマット用の基礎情報、前記他のフォーマット用の署名データを取得し、取得した情報及び署名データに基づいて前記一のフォーマット用の公開鍵証明書を作成する過程を含む、

公開鍵証明書の発行方法。

【請求項３】　請求項１又は２記載の発行方法により発行された公開鍵証明書から前記各基礎情報及び署名データを取り出して当該公開鍵証明書の正当性を検証する装置において実行される方法であって、

前記取り出した各基礎情報をそれが対応するフォーマット以外の他のフォーマットに変換することで当該他のフォーマットに対応する基礎情報を生成し、前記公開鍵証明書から取り出した基礎情報又は前記他のフォーマットに対応する基礎情報と前記公開鍵証明書から取り出した複数の署名データのいずれかとが合致する場合に、前記公開鍵証明書を正当と判断することを特徴とする、

公開鍵証明書の検証方法。

【請求項４】　所定の申請情報に基づいて生成された公開鍵証明書用の複数の基礎情報をすべてのフォーマットに共通の基礎情報と各フォーマットに固有の基礎情報とに分類する基礎情報生成手段と、

前記共通の基礎情報及び一のフォーマットに固有の基礎情報を対象とした当該一のフォーマット用の署名データを生成する署名手段と、

前記生成した基礎情報及び署名データと、他のフォーマットに固有の基礎情報と、前記一のフォーマット及び他のフォーマットに共通の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて前記他のフォーマット用の公開鍵証明書を作成する発行手段とを有し、

一のフォーマットと他のフォーマットのいずれにも対応可能な公開鍵証明書を発行することを特徴とする、

公開鍵証明書発行装置。

【請求項５】　所定の申請情報に基づいて複数フォーマットに対応可能な公開鍵証明書を発行する第１装置と、発行された公開鍵証明書を独自フォーマットの公開鍵証明書に変換する第２装置とを有し、

第１装置は、

2

前記申請情報に基づいて生成された公開鍵証明書用の複数の基礎情報をすべてのフォーマットに共通の基礎情報と各フォーマットに固有の基礎情報に分類する基礎情報生成手段と、

前記共通の基礎情報及び一のフォーマットに固有の基礎情報を対象とした当該一のフォーマット用の署名データを生成する署名手段と、

前記生成した基礎情報及び署名データと、他のフォーマットに固有の基礎情報と、前記一のフォーマット及び他のフォーマットに共通の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて前記他のフォーマット用の公開鍵証明書を作成する公開鍵証明書発行手段とを有し、

第２装置は、

前記他のフォーマット用の公開鍵証明書から前記共通の基礎情報、前記一のフォーマットに固有の基礎情報、前記一のフォーマット用の署名データ、前記他のフォーマットに固有の基礎情報及び前記他のフォーマット用の署名データを取得し、取得した情報及びデータに基づいて前記一のフォーマット用の公開鍵証明書を作成する手段を有することを特徴とする、

公開鍵証明書発行システム。

【請求項６】　第２装置は、前記一のフォーマット用の公開鍵証明書を検証した後、その公開鍵証明書を所定の情報記録媒体に格納するように構成されていることを特徴とする、請求項５記載の公開鍵証明書発行システム。

【請求項７】　第１装置及び第２装置の少なくとも一方が、ネットワークに接続されたプロキシ装置で構成されていることを特徴とする、

請求項５記載の公開鍵証明書発行システム。

【請求項８】　所定の申請情報に基づいて生成された公開鍵証明書用の複数のフォーマットの基礎情報を所定順に配列するとともに、各基礎情報の各々のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成し、

申請者側で利用可能なフォーマットに対応する基礎情報と、この基礎情報のフォーマット以外の他のフォーマットの基礎情報から生成したハッシュ値と、前記生成された署名データとを含めて公開鍵証明書を作成する過程を含む、

公開鍵証明書の発行方法。

【請求項９】　請求項８記載の発行方法により発行された公開鍵証明書から前記基礎情報、前記複数のハッシュ値及び署名データを取り出す過程と、

取り出した基礎情報をハッシュしてハッシュ値を生成するとともに、生成したハッシュ値と前記公開鍵証明書から取り出したハッシュ値とを連結して連結ハッシュ値を生成する過程と、

生成した連結ハッシュ値と前記公開鍵証明書から取り出した署名データとを比較する過程とを含み、

署名データと連結ハッシュ値とが合致する場合に前記公開鍵証明書を正当と判断することを特徴とする、
公開鍵証明書の検証方法。

【請求項１０】　所定の申請情報に基づいて生成された公開鍵証明書用の複数のフォーマットの基礎情報を所定順に配列する基礎情報配列手段と、
複数の基礎情報の各々のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成する署名手段と、
申請者側で利用可能なフォーマットに対応する基礎情報、該フォーマットに対応する基礎情報以外の基礎情報から生成したハッシュ値及び前記生成した署名データを含めて公開鍵証明書を作成する発行手段とを有し、
複数のフォーマットに対応可能な一つの公開鍵証明書を発行することを特徴とする、公開鍵証明書発行装置。

【請求項１１】　所定の申請情報に基づいて公開鍵証明書用の複数の基礎情報を用意する処理、
前記複数の基礎情報のうち一のフォーマット用の基礎情報を対象とした当該一のフォーマット用の署名データを生成する処理、
前記生成した基礎情報及び署名データと他のフォーマット用の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて前記他のフォーマット用の公開鍵証明書を作成する処理をコンピュータに実行させるためのプログラムコードが記録された、コンピュータ読みとり可能な記録媒体。

【請求項１２】　所定の申請情報に基づいて公開鍵証明書用の複数のフォーマットの基礎情報を生成する処理、
前記複数のフォーマットの基礎情報の各々ハッシュ値を生成する処理、
生成された複数のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成する処理、
申請者側で利用可能なフォーマットに対応する基礎情報と、この基礎情報のフォーマット以外の他のフォーマットの基礎情報から生成したハッシュ値と、前記生成された署名データとを含めて公開鍵証明書を作成する処理をコンピュータに実行させるためのプログラムコードが記録された、コンピュータ読みとり可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、汎用のメディア用の標準のフォーマットとリソースの小さなメディアに適した独自のフォーマットのいずれにも対応可能な公開鍵証明書を発行する技術、及び発行された公開鍵証明書の検証技術に関する。メディアとは公開鍵証明書を利用する情報処理手段（端末、ＩＣカード等）であり、フォーマットとは、メディアが解釈可能な公開鍵証明書の規格をいう。

〔発明の詳細な説明〕

【０００２】

【発明の背景】近年、電子メールシステム、電子マネー

システム、電子決済システム、電子商取引システム、電子申請システム等のネットワークを利用した様々なシステムが実用化されている。このようなシステムでは通信の秘匿性が非常に重要になることから暗号化技術が応用されているが、現在は、暗号鍵や復号鍵を保守するにあたっての労力が小さくて済むという利点を持つ公開鍵暗号方式が広く用いられるようになっている。

【０００３】公開鍵暗号方式では、その公開鍵の持ち主を証明するために、公共性の強い認証局と呼ばれる機関が認証局による署名データ入りの公開鍵証明書を発行するのが一般的である。公開鍵証明書には、多種多様な目的や用途に対して柔軟に対応することがその性質上求められているが、従来は、そのフォーマットに様々な項目を含めることによってその汎用性を確保している。例えば、公開鍵証明書の標準となっているＩＴＵ－Ｔ（国際電気通信連合電気通信標準化部門）の「Ｘ５０９」は、非常に多くの項目を含んでおり、その内容がかなり複雑なものとなっている。このような複雑な内容の公開鍵証明書は、その汎用性ゆえに非常に魅力的なものとなっているが、その反面、これをＩＣカード等のようなリソースの少ないものに応用する場合は難点がある。

【０００４】即ち、リソースの小さいＩＣカード等では、汎用性の高い上記のような一般的な公開鍵証明書を取り扱うには、プログラムサイズの増大、処理時間の増加、メモリの圧迫といった問題が発生し、そのまま利用できない場合が生じる。このような場合には、特定サービス限定の独自フォーマットを採用することが考えられるが、そのためには、汎用性のある公開鍵証明書用のインフラ以外の専用インフラを構築することが必要となるが、これは、その手間やコストの面から見て必ずしも妥当な解決手段とはいえない。

【０００５】もし、ＩＣカード等のリソースの小さなものに、ＩＴＵ－Ｔ「Ｘ５０９」等の汎用性の高いフォーマットを採用した場合、或いはＩＣカード内部で汎用フォーマットを独自フォーマットに変換し、これを保管することにした場合、上記のような難点を理論上は解消できるが、ＩＣカードの限られたリソースが、フォーマットの解釈や変換機能を実現するために消費されてしまい、そもそも実装できないか、本来達成しようとしていた機能を十分に達成できない事態が生じる。

【０００６】本発明は、標準のフォーマットにも対応することができ、且つリソースの小さなメディアでの使用にも適した汎用性の高い公開鍵証明書の発行方法、発行装置、発行システムを提供することをその主たる課題とするものである。本発明は、また、公開鍵証明書の検証を適切に行うことができる検証方法及び、公開鍵証明書の発行方法を汎用のコンピュータ上で実現する上で好適となる記録媒体を提供することをその課題とする。

【０００７】

【課題を解決するための手段】本発明は、上記課題を解

決するために以下に説明するような２通りの公開鍵証明書の発行方法を提供する。第１の公開鍵証明書の発行方法は、所定の申請情報に基づいて生成された公開鍵証明書用の複数の基礎情報のうち、一のフォーマット用の基礎情報を対象とした当該一のフォーマット用の署名データを生成するとともに、前記生成した基礎情報及び署名データと、他のフォーマット用の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて前記他のフォーマット用の公開鍵証明書を作成する。また、作成された公開鍵証明書から前記一のフォーマット用の基礎情報、前記一のフォーマット用の署名データ、前記他のフォーマット用の基礎情報、前記他のフォーマット用の署名データを取得し、取得した情報及び署名データに基づいて前記一のフォーマット用の公開鍵証明書を作成する。このような過程を含む公開鍵証明書の発行方法である。

【０００８】この方法により発行された公開鍵証明書は、以下のようにして検証することができる。まず、公開鍵証明書から各基礎情報及び署名データを取り出し、必要な場合に、取り出した各基礎情報をそれが対応するフォーマット以外の他のフォーマットに変換することで当該他のフォーマットに対応する基礎情報を生成し、公開鍵証明書から取り出した基礎情報又は前記他のフォーマットに対応する基礎情報と公開鍵証明書から取り出した複数の署名データのいずれかとが合致する場合に、その公開鍵証明書を正当と判断する。

【０００９】フォーマットの変換を行った場合は、基礎情報と署名データとの間における照合を行えなくなるのが通常である。しかしながら、この発明で発行される公開鍵証明書には、複数の署名データが含まれており、且つこの署名データは、他のフォーマットに変換した基礎情報を署名対象として生成されているので、フォーマット変換後においても照合が可能になる。また、フォーマット変換を前提とすることにより、特定サービス／アプリケーションに最適化した基礎情報のフォーマットを採用しても、独自フォーマット専用のインフラを構築する必要がなくなる。

【００１０】上記の公開鍵証明書の発行方法は、例えば、以下のように構成される公開鍵証明書発行装置又はシステムによってその実行が可能である。公開鍵証明書発行装置は、所定の申請情報に基づいて生成された公開鍵証明書用の複数の基礎情報をすべてのフォーマットに共通の基礎情報と各フォーマットに固有の基礎情報とに分類する基礎情報生成手段と、前記共通の基礎情報及び一のフォーマットに固有の基礎情報を対象とした当該一のフォーマット用の署名データを生成する署名手段とを有し、さらに、生成した基礎情報及び署名データ、他のフォーマットに固有の基礎情報、一のフォーマット及び他のフォーマットに共通の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて他のフォーマット用の公開鍵証明書を作成する発行手段とを有し、一のフォーマットと他のフォーマットのいずれにも対応可能な公開鍵証明書を発行する装置である。

【００１１】公開鍵証明書発行システムは、所定の申請情報に基づいて複数フォーマットに対応可能な公開鍵証明書を発行する第１装置と、発行された公開鍵証明書を独自フォーマットの公開鍵証明書に変換する第２装置とを含んで構成される。第１装置は、申請情報に基づいて生成された公開鍵証明書用の複数の基礎情報をすべてのフォーマットに共通の基礎情報と各フォーマットに固有の基礎情報に分類する基礎情報生成手段と、前記共通の基礎情報及び一のフォーマットに固有の基礎情報を対象とした当該一のフォーマット用の署名データを生成する署名手段と、生成した基礎情報及び署名データと他のフォーマットに固有の基礎情報と一のフォーマット及び他のフォーマットに共通の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて他のフォーマット用の公開鍵証明書を作成する公開鍵証明書発行手段とを有するものであり、第２装置は、他のフォーマット用の公開鍵証明書から共通の基礎情報、一のフォーマットに固有の基礎情報、一のフォーマット用の署名データ、他のフォーマットに固有の基礎情報及び他のフォーマット用の署名データを取得し、取得した情報及びデータに基づいて一のフォーマット用の公開鍵証明書を作成する手段を有するものである。第２装置は、例えば、一のフォーマット用の公開鍵証明書を検証した後、その公開鍵証明書を所定の情報記録媒体に格納するように構成される。なお、第１装置及び第２装置は、例えばネットワークを介して接続された独立の装置であっても良く、第１装置及び第２装置の少なくとも一方の機能を同一の情報処理装置又はシステム内で構築しても良い。後者の場合、その情報処理装置又はシステムをプロキシ（proxy）装置とすることで、外部に隠蔽された状態で本発明の公開鍵証明書発行方法を実現することができる。また、このプロキシ装置に、既存の公開鍵発行システムにない部分のみを配置し、既存の公開鍵発行システムと共同で公開鍵証明書を発行するようにすることで、本発明の実施がより容易となる。

【００１２】次に、第２の公開鍵証明書の発行方法について説明する。この方法は、所定の申請情報に基づいて生成された公開鍵証明書用の複数のフォーマットの基礎情報を所定順に配列するとともに、各基礎情報の各々のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成し、申請者側で利用可能なフォーマットに対応する基礎情報と、この基礎情報のフォーマット以外の他のフォーマットの基礎情報から生成したハッシュ値と、生成された署名データとを含めて公開鍵証明書を作成する過程を含む方法である。ハッシュ値の連結は、複数のハッシュ値の論理条件を判定することにより行う。第１の公開鍵証明書発行方法と比較して第２の公開鍵証

明書の発行方法は、それにより得られる公開鍵証明書のデータ量を小さくすることができる。これは、ハッシュ値のデータ量が、署名データのデータ量よりも小さいことに基く。

【００１３】この発行方法により発行された公開鍵証明書の検証は、以下のようにして行われる。即ち、検証を行う装置において、公開鍵証明書から基礎情報、複数のハッシュ値及び署名データを取り出す過程と、取り出した基礎情報をハッシュしてハッシュ値を生成するとともに、生成したハッシュ値と前記公開鍵証明書から取り出したハッシュ値とを連結して連結ハッシュ値を生成する過程と、生成した連結ハッシュ値と前記公開鍵証明書から取り出した署名データとを比較する過程とをこの順に実行し、署名データと連結ハッシュ値とが合致する場合に公開鍵証明書を正当と判断する。

【００１４】第２の公開鍵証明書の発行方法は、例えば以下のような公開鍵証明書発行装置において実施することができる。この公開鍵証明書発行装置は、所定の申請情報に基づいて生成された公開鍵証明書用の複数のフォーマットの基礎情報を所定順に配列する基礎情報配列手段と、複数の基礎情報の各々のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成する署名手段と、申請者側で利用可能なフォーマットに対応する基礎情報、該フォーマットに対応する基礎情報以外の基礎情報から生成したハッシュ値及び生成した署名データを含めて公開鍵証明書を作成する発行手段とを有し、複数のフォーマットに対応可能な一つの公開鍵証明書を発行することを特徴とするものである。

【００１５】第１及び第２の公開鍵証明書の発行方法を汎用のコンピュータ上で実行する上で用いる記録媒体は、それぞれ以下のようなものである。第１の公開鍵証明書の発行方法をコンピュータ上で実現するための記録媒体は、コンピュータに下記の処理を実行させるためのプログラムが記録されたコンピュータ読みとり可能な記録媒体である。

（１－１）所定の申請情報に基づいて公開鍵証明書用の複数の基礎情報を用意する処理、（１－２）前記複数の基礎情報のうち一のフォーマット用の基礎情報を対象とした当該一のフォーマット用の署名データを生成する処理、（１－３）生成した基礎情報及び署名データと、他のフォーマット用の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて他のフォーマット用の公開鍵証明書を作成する処理。

【００１６】第２の公開鍵証明書の発行方法をコンピュータ上で実現するための記録媒体は、コンピュータに下記の処理を実行させるためのプログラムが記録されたコンピュータ読みとり可能な記録媒体である。

（２－１）所定の申請情報に基づいて公開鍵証明書用の複数のフォーマットの基礎情報を生成する処理、（２－２）複数のフォーマットの基礎情報の各々ハッシュ値を生成する処理、（２－３）生成された複数のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成する処理、（２－４）申請者側で利用可能なフォーマットに対応する基礎情報と、この基礎情報のフォーマット以外の他のフォーマットの基礎情報から生成したハッシュ値と、前記生成された署名データとを含めて公開鍵証明書を作成する処理。

【００１７】

【発明の実施の形態】以下、図面を参照して、本発明による公開鍵証明書発行方法、検証方法、発行システムの実施の形態を説明する。ここでは、標準フォーマットであるＩＴＵ－Ｔ「Ｘ５０９」と、リソースの小さなＩＣカード用の単純なフォーマット「ＥＭＶ」との間の互換が可能な公開鍵証明書の例を挙げる。

【００１８】（第１実施形態）まず、第１の公開鍵証明書発行方法の実施の形態を説明する。図１は、この方法の実施に適した公開鍵証明書サービスシステムの構成図である。この公開鍵証明書サービスシステム１は、フォーマットの互換性を有する公開鍵証明書を発行する機能を有する認証局４０、上記公開鍵証明書を独自フォーマットの公開鍵証明書に変換する機能を有する端末１０、端末１０によってフォーマット変換された公開鍵証明書を保持するとともにサーバ３０の公開鍵証明書の検証機能を有するＩＣカード２０、ＩＣカード２０の公開鍵証明書の検証機能を有すサーバ３０を、それぞれ双方向通信可能な環境のネットワークＮに接続して構成される。

【００１９】端末１０は、ＩＣカード２０との間で情報の授受を行うリーダライタ１４を有する一種のコンピュータである。この端末１０は、図示しないコンピュータのＣＰＵが自己のオペレーティングシステム下で所定のプログラムを読み込んで実行することにより形成されるデータ処理部１１、通信制御部１２、及び検証処理部１３とを含んで構成される。データ処理部１１は、ＩＣカード２０等との間でデータのやりとりを行ったり所定の変換アルゴリズムに従って公開鍵証明書のフォーマット変換等を行うものであり、通信制御部１２は、ネットワークを経由する情報の制御を行うものである。検証処理部１３は、公開鍵証明書等の検証を行うものである。

【００２０】ＩＣカード２０は、端末１０等との間でデータのやりとりを行うデータ処理部２１、公開鍵証明書の検証を行う検証処理部２２、及び自己の公開鍵証明書や検証済みの公開鍵等を格納するデータ格納部２３を含んで構成される。これらのデータ処理部２１、検証処理部２２、データ格納部２３は、図示しないＲＯＭ内のプログラムをＣＰＵが実行することにより形成される。

【００２１】サーバ３０は、端末１０や認証局４０との間でデータのやりとりを行うデータ処理部３１、ネットワークＮからの情報を制御する通信制御部３２、公開鍵証明書の検証を行う検証処理部３３、及び検証した公開鍵証明書や公開鍵等を格納するデータ格納部３４を含ん

で構成されている。

【００２２】認証局４０は、コンピュータないしコンピュータシステムによって実現されるもので、コンピュータ等のＣＰＵが自己のオペレーティングシステム下で所定のプログラムを読み込んで実行することにより形成される各種機能ブロック、即ち、ネットワークＮからの情報を制御する通信制御部４１、公開鍵証明書の発行や生成を管理する公開鍵証明書発行部４２、各々異なるフォーマットの基礎情報を管理する第１基礎情報管理部４３及び第２基礎情報管理部４４を含んで構成されている。公開鍵証明書発行部４２は、申請者からの申請情報に基づいて公開鍵証明書用の基礎情報を生成する基礎情報生成部４２ａと、基礎情報を対象とした署名データを生成する署名部４２ｂと、基礎情報及び署名データを含めて公開鍵証明書を作成（発行）する発行部４２ｃとを含んでいる。

【００２３】次に、上記のように構成される公開鍵証明書サービスシステムの動作を説明する。まず、認証局４０において公開鍵証明書を発行する場合の手順を図２を参照して説明する。ここでは、あとでＩＣカード２０用のＥＭＶフォーマットに変換されることを考慮したＸ５０９フォーマットの公開鍵証明書を発行するものとする。以後の説明では、フォーマットの種類を区別する必要がある場合において、Ｘ５０９フォーマットを「Ｘ５０９」、ＥＭＶフォーマットを「ＥＭＶ」と表現する。また、各フォーマットの公開鍵証明書に記述すべき項目のうち、Ｘ５０９とＥＭＶに共通の項目をＣ、Ｘ５０９のみに必要な項目をＡ、ＥＭＶのみに必要な項目をＢとする。

【００２４】認証局４０の公開鍵証明書発行部４２は、例えば端末１０から公開鍵証明書の申請情報を受け取ると（ステップＳ１０１）、この申請情報に基づいてＸ５０９、ＥＭＶに対応する項目（Ａ、Ｂ、Ｃ）を作成ないし分類し、第２基礎情報管理部４４に、項目Ｃ及び項目Ｂを対象としたＥＭＶ用の署名データＳＩＧＮ＃２を生成させる（ステップＳ１０２）。公開鍵証明書発行部４２は、また、項目Ｂと上記署名データＳＩＧＮ＃２を公開鍵証明書の拡張領域に格納するデータ（「拡張データ」）ＡＰＤＸ＃２として、第１基礎情報管理部４３に、項目Ｃ、項目Ａ、及び拡張データＡＰＤＸ＃２を対象としたＸ５０９用の署名データＳＩＧＮ＃１を生成させる（ステップＳ１０３）。

【００２５】その後、項目Ｃ、項目Ａ、及びＸ５０９用の署名データＳＩＧＮ＃１を含んだＸ５０９公開鍵証明書を発行し（ステップＳ１０４）、これを通信制御部４１を通して端末１０宛に送付する。このようにして発行されたＸ５０９公開鍵証明書は、ＩＣカード２０において使用できるようにするため、端末１０でＥＭＶ公開鍵証明書に変換される。具体的には、Ｘ５０９公開鍵証明書から項目Ｃ及び項目Ｂを取得してこれをＥＭＶの基礎情報ＤＡＴＡ＃２とする。また、拡張データＡＰＤＸ＃２からＥＭＶ用の署名データＳＩＧＮ＃２を取得し、さらに項目Ａ及びＸ５０９用の署名データＳＩＧＮ＃１を取得してＥＭＶ公開鍵証明書に変換する。このようにして変換されたＥＭＶ公開鍵証明書は、端末１０又はサーバ３０で何時でもＸ５０９公開鍵証明書に変換できるようになっている。

【００２６】図３は、Ｘ５０９公開鍵証明書とＥＭＶ公開鍵証明書の項目の対応関係を概念的に示した図である。認証局４０から発行されたＸ５０９公開鍵証明書は、図３左側に示されるように、基本情報領域と基本署名領域とを有している。基本情報領域には、項目Ｃ、項目Ａ、拡張データ（項目Ｂ及び署名データＳＩＧＮ＃２）ＡＰＤＸ＃２が格納される。これらの格納情報がＸ５０９用の基礎情報ＤＡＴＡ＃１となり、この基礎情報ＤＡＴＡ＃１を対象とした署名データＳＩＧＮ＃１が、基本署名領域に格納されるようになっている。

【００２７】一方、ＥＭＶ公開鍵証明書は、図右側に示されるように、その基本情報領域に、項目Ｃ及び項目Ｂのみが格納され、これらがＥＭＶ用の基礎情報ＤＡＴＡ＃２となる。そして、この基礎情報ＤＡＴＡ＃２を対象とした署名データＳＩＧＮ＃２が基本署名領域に格納されるようになっている。ＥＭＶ公開鍵証明書の付属データ領域には、項目Ａ及びＸ５０９用の署名データＳＩＧＮ＃１が、付属データＡＰＤＸ＃１として格納されるようになっている。

【００２８】次に、各公開鍵証明書の検証処理について説明する。Ｘ５０９公開鍵証明書の検証処理は、Ｘ５０９用の署名データＳＩＧＮ＃１が基礎情報ＤＡＴＡ＃１についての正しい署名データになっているかどうかを確認する処理であり、ＥＭＶ公開鍵証明書の検証処理は、ＥＭＶ用の署名データＳＩＧＮ＃２が基礎情報ＤＡＴＡ＃２についての正しい署名データになっているかどうかを確認する処理である。

【００２９】フォーマット変換を行った場合は署名データの照合を行えなくなるのが通常であるが、本実施形態の公開鍵証明書には、二種類のフォーマットによる署名データＳＩＧＮ＃１、ＳＩＧＮ＃２が含まれており、しかもこれらの署名データのうち一方のフォーマットに対応するものは、他方のフォーマットに変換した基礎情報を署名対象として生成されたものとなっているので、フォーマット変換後においても照合等を行うことが可能になる。つまり、使用が予想されるフォーマットに変換した基礎情報を対象として生成した署名データを、複数の署名データの一つに含めて公開鍵証明書を作成しておけば、基礎情報とそれに基いて作成された署名データとを照合することは、フォーマット変換後においても可能となる。

【００３０】このように、本実施形態により発行される公開鍵証明書は、汎用性の高いＸ５０９フォーマット

と、ＩＣカード２０のようにリソースが小さいものにおいて利用し易いＥＭＶフォーマットの両方に対応することができるので、フォーマット毎のインフラを別途構築する必要がなくなり、公開鍵証明書を利用するシステムの構成が簡略化される利点がある。

【００３１】また、フォーマット変換を要する公開鍵証明書の検証処理は、リソースの大きな端末１０が行い、ＩＣカード２０へは正当性が確認された公開鍵証明書を格納することで、ＩＣカード２０側で、フォーマット変換のために限られたリソースを無駄に使用することもなくなる。

【００３２】以上、Ｘ５０９フォーマットとＥＭＶフォーマットの両方に対応できる公開鍵証明書の発行、検証の例を示したが、一つの公開鍵証明書で３種類以上のフォーマットに対応できるようにすることも可能である。例えば図４は、４通りのフォーマット(フォーマット＃１、フォーマット＃２、フォーマット＃３、フォーマット＃４)に対応できるようにした公開鍵証明書の概念図である。基礎情報ＤＡＴＡ＃１から基礎情報ＤＡＴＡ＃４までの双方向のフォーマット変換は、リソースの大きなワークステーションで行い、リソースの小さいＩＣカードでは、フォーマットの内容チェックやフォーマット変換を要しない検証のみを行う。

【００３３】図４のように４通りのフォーマットに対応させる場合、ある一つのフォーマット、例えばフォーマット＃１における基礎情報ＤＡＴＡ＃１とこの基礎情報ＤＡＴＡ＃１を他のフォーマットに変換した基礎情報（ＤＡＴＡ＃２、ＤＡＴＡ＃３、ＤＡＴＡ＃４）について生成した署名データを計４個（ＳＩＧＮ＃１、ＳＩＧＮ＃２、ＳＩＧＮ３、ＳＩＧＮ４）作成する。

【００３４】なお、一つのフォーマットについての署名データを生成する際に、他のフォーマットで生成した署名データをも含めて署名対象とする方法としない方法とがある。前者の方法は、図４のフォーマット＃１の例では、基礎情報ＤＡＴＡ＃１のほかに、他の署名データＳＩＧＮ＃２、ＳＩＧＮ＃３、ＳＩＧＮ＃４を対象として署名データＳＩＧＮ＃１を作成する方法であり、後者の方法は、基礎情報ＤＡＴＡ＃１のみを署名対象として署名データＳＩＧＮ＃１を生成する方法である。

【００３５】公開鍵証明書の基礎情報領域は、４つのパターンのいずれかにより表現されるので、ＩＣカードに読み込ませる場合には、所定のフォーマット変換ルールに従って、必要なフォーマットに変換した後に読み込ませることになる。例えば公開鍵証明書の基礎情報がフォーマット＃１で表現されたＤＡＴＡ＃１であり、ＩＣカードにおいてフォーマット＃２で検証する場合は、基礎情報ＤＡＴＡ＃１をフォーマット＃２に変換した基礎情報ＤＡＴＡ＃２内の署名データが、それに対応した署名データＳＩＧＮ＃２になっていることを確認する。フォーマット＃２以外のフォーマットに変換する際も同様である。

【００３６】（第２実施形態）次に、第２の公開鍵証明書の発行方法の実施の形態を説明する。この方法を実施するためのシステム構成は、図１に示した公開鍵証明書サービスシステムとほぼ同様である。但し、この実施形態の公開鍵証明書サービスシステムは、認証局の構成が第１実施形態のサービスシステム１のものと異なる。本実施形態の認証局４００は、図５に示した通り、通信制御部４１０、公開鍵証明書発行部４２０及び署名部４３０を有している。

【００３７】公開鍵証明書発行部４２０は、公開鍵証明書発行の申請情報に基づいて複数のフォーマットに対応する基礎情報を生成する基礎情報生成部４２０ａと、生成された基礎情報の各々をハッシュして複数のハッシュ値を生成するハッシュ部４２０ｂと、申請者で利用可能なフォーマットに対応する基礎情報と該基礎情報以外の基礎情報から生成したすべてのハッシュ値と上記署名データとを含めて公開鍵証明書を作成（発行）する発行部４２０ｃを含んで構成されるものである。

【００３８】まず、この認証局４００において、第１実施形態と同様、Ｘ５０９とＥＭＶの互換性がある公開鍵証明書を発行する場合の動作を説明する。この実施形態では、Ｘ５０９（フォーマット＃１）で表現された基礎情報をＤＡＴＡ＃１、ＥＭＶ（フォーマット＃２）で表現された基礎情報をＤＡＴＡ＃２とする。

【００３９】基礎情報ＤＡＴＡ＃１は、ＥＭＶのみに必要な項目Ｂを別領域である拡張データとし、項目Ｃ，項目Ａ，項目Ｂの順に並べて構築される。Ｃは、共通の項目である。基礎情報ＤＡＴＡ＃２は、Ｘ５０９のみに必要な項目Ａを別領域である付属データとして、項目Ｃ，項目Ｂ，項目Ａの順に並べて構築される。

【００４０】認証局４００では、まず、ｈ（ｘ）を一方向性ハッシュ関数とし、ハッシュ値Ｈ１＝ｈ（Ｃ，Ａ）、ハッシュ値Ｈ２＝ｈ（Ｃ，Ｂ）を定義する。そして、これら２つのハッシュ値Ｈ１、Ｈ２を連結した連結ハッシュ値を署名対象として認証局４００の基本署名データを生成する。そして、基礎情報ＤＡＴＡ＃１、ハッシュ値Ｈ２、基本署名データを含むＸ５０９公開鍵証明書を発行する。ＥＭＶ公開鍵証明書については、基礎情報ＤＡＴＡ＃２、ハッシュ値Ｈ１、基本署名データを含むものとして発行する。

【００４１】具体的には、図６のフローチャートに示したような手順により、公開鍵証明書の発行がなされる。即ち、端末１０から公開鍵証明書発行の申請情報を受け取ると（ステップＳ２０１）、公開鍵証明書発行部４２は、各フォーマットに対応する項目（Ａ、Ｂ、Ｃ）を生成するとともに、ハッシュ関数ｈ（ｘ）を用いてハッシュ値Ｈ１＝ｈ（Ｃ，Ａ）及びＨ２＝ｈ（Ｃ，Ｂ）を求める（ステップＳ２０２）。

【００４２】次に、ハッシュ値Ｈ１とハッシュ値Ｈ２と

を連結した連結ハッシュ値（Ｈ１｜Ｈ２）を対象として署名データＳＩＧＮを生成する（ステップＳ２０３）。公開鍵証明書発行部４２は、また、項目Ｃと項目Ａを拡張データとし、項目Ｂとハッシュ値Ｈ２、基本署名データを含んだＸ５０９公開鍵証明書を発行し（ステップＳ２０４）、これを通信制御部４１０を通して端末１０宛に送付する。

【００４３】このＸ５０９公開鍵証明書をＥＭＶ公開鍵証明書に変換する場合は、ＥＭＶの基礎情報ＤＡＴＡ＃２を｛Ｃ，Ｂ，Ａ｝、ハッシュ値Ｈ１をｈ（Ｃ，Ａ）に変換する。一方、ＥＭＶ公開鍵証明書をＸ５０９公開鍵証明書に変換する場合は、Ｘ５０９の基礎情報ＤＡＴＡ＃１を｛Ｃ，Ａ，Ｂ｝、ハッシュ値Ｈ２をｈ（Ｃ，Ａ）に変換する。

【００４４】各公開鍵証明書の検証処理は、Ｘ５０９の場合は項目Ｃと項目Ａからハッシュ値Ｈ１を求め、基本署名データＳＩＧＮが連結ハッシュ値（Ｈ１｜Ｈ２）についての正しい署名データになっているかを確認することにより行う。一方、ＥＭＶの場合は、項目Ｃと項目Ｂからハッシュ値Ｈ２を求め、基本署名データＳＩＧＮが連結ハッシュ値（Ｈ１｜Ｈ２）についての正しい署名データになっているかを確認することにより行う。

【００４５】次に、第１実施形態の場合と同様、４通りのフォーマット(フォーマット＃１、フォーマット＃２、フォーマット＃３、フォーマット＃４)に対応できるようにした公開鍵証明書の例を説明する。図７は、この実施形態によるフォーマット変換の概念図である。

【００４６】まず、フォーマット＃１での基礎情報ＤＡＴＡ＃１と他の３つのフォーマットで表現された基礎情報（ＤＡＴＡ＃２、ＤＡＴＡ＃３、ＤＡＴＡ＃４）をハッシュ関数で求めた３つのハッシュ値（ＨＡＳＨ＃２、ＨＡＳＨ＃３、ＨＡＳＨ＃４）と、これらの３つのハッシュ値を連結した連結ハッシュ値を署名対象として生成した一つの基本署名データ（ＳＩＧＮ）とを用意する。第１実施形態の場合と同様に、公開鍵証明書の基礎情報領域は、４つのいずれかのパターンで表現されるので、ＩＣカード２０に読み込ませる場合には、フォーマット変換ルールに従って、必要なフォーマットに変換した後に読み込ませることが可能である。

【００４７】フォーマットの変換は、次のようにして行うことができる。例えばフォーマット＃１からフォーマット＃２に変換する場合を考える。この場合は、まず、フォーマット＃１の基礎情報ＤＡＴＡ＃１のハッシュ値ＨＡＳＨ＃１を作る。次に、基礎情報ＤＡＴＡ＃１を変換してフォーマット＃２の基礎情報ＤＡＴＡ＃２を作る。変換前のハッシュ値ＨＡＳＨ＃２は不要となるので、捨てる。記憶領域に余裕がある場合は捨てなくとも良いが、基礎情報ＤＡＴＡ＃２とハッシュ値ＨＡＳＨ＃２とが整合していることの確認は必要である。フォーマット＃２を検証する場合は、基礎情報ＤＡＴＡ＃２をハッシュしてハッシュ値ＨＡＳＨ＃２を求め、ＨＡＳＨ＃１からＨＡＳＨ＃４までを連結したものを署名対象として基本署名データＳＩＧＮを生成し、それが正しい署名データであるかどうかを確認する。

【００４８】各ハッシュ値は、各々のフォーマットでの基礎情報をフォーマット変換できれば何時でも再生が可能なので、ＩＣカード等のようなデバイスでは、検証処理後はそれらを保存する必要はなく、記憶領域を少なくすることができる。例えば図示のようにフォーマット＃２の場合、検証処理後は、各ハッシュ値ＨＡＳＨ＃１、ＨＡＳＨ＃３，ＨＡＳＨ＃４は捨てることが可能である。この場合、他のフォーマットに変換する際に、フォーマット＃１～フォーマット＃４まで順番にフォーマット変換してＨＡＳＨ＃１～ＨＡＳＨ＃４を再生することになる。

【００４９】この実施形態による公開鍵証明書の発行方法では、第１実施形態が４つの署名データが必要となるのに対し、一つの基本署名データと３つのハッシュ値が必要となる。通常、署名データは、ハッシュ値よりもかなり大きくなるので、この実施形態の方が、保存するデータ量は少なくて済む。

【００５０】また、第１実施形態及び第２実施形態では、認証局４０が新規な構成要素を備えて構成される場合の例を説明したが、各実施形態の認証局４０、４００の機能をもった情報処理装置ないしシステムをネットワークＮ上に配置し、この情報処理装置ないしシステムを通じて上記機能ないし処理を実現しても良い。特に、情報処理装置ないしシステムをプロキシサーバで構成することで、外部から隠蔽された状態で公開鍵証明書を発行できるようになる。

【００５１】

【実施例】次に、本発明の実施例を説明する。図８は、サーバ３０とＩＣカード２０との間で、端末１０を介して相互に公開鍵証明書を検証するとともに、正当な場合に各々の公開鍵を相手に渡して暗号通信を行えるようにする場合シーケンスチャートである。図８において、ＥＭＶ－ＣＥＲＴ＃１は、ＩＣカード２０が保有する公開鍵＃１の正当性を証明するための公開鍵証明書、Ｘ５０９－ＣＥＲＴ＃１は、端末１０において利用可能なＸ５０９公開鍵証明書、Ｘ５０９－ＣＥＲＴ＃２はサーバ３０が保有する公開鍵＃２の正当性を証明するためのＸ５０９公開鍵証明書、ＥＭＶ－ＣＥＲＴ＃２は、Ｘ５０９－ＣＥＲＴ＃２を変換したＥＭＶ公開鍵証明書である。

【００５２】ＩＣカード２０を保有する利用者は、そのＩＣカード２０を端末１０のリーダライタ１４に装着する。ＩＣカード２０が装着されると、端末１０は、ＩＣカード２０からＥＭＶ－ＣＥＲＴ＃１（ＥＭＶのフォーマットで基礎情報領域が生成されている）を受領し、これをデータ処理部１１でＸ５０９－ＣＥＲＴ＃１に変換する（Ｔ３０１）。その後、検証処理部１３でＸ５０９

15

－ＣＥＲＴ＃１の検証処理を行い（Ｔ３０２）、そのＸ５０９－ＣＥＲＴ＃１が正当と判断できる場合は公開鍵＃１を格納する（Ｔ３０３）。データ処理部１１は、リーダライタ１４を介してＩＣカード２０に検証終了信号を送信する。端末１０は、また、ＩＣカード２０からＸ５０９－ＣＥＲＴ＃１をサーバ３０に送信する要求を受領すると、端末１０は、Ｘ５０９－ＣＥＲＴ＃１をサーバ３０宛に送付する。

【００５３】Ｘ５０９－ＣＥＲＴ＃１を受領したサーバ３０は、検証処理部３３でＸ５０９－ＣＥＲＴ＃１の検証処理を行う（Ｓ３０１）。正当と判断できる場合は、データ格納部３４に公開鍵＃１を格納する（Ｓ３０２）。また、データ格納部３４に格納されているＸ５０９－ＣＥＲＴ＃２を端末宛１０宛に送信する。サーバ３０からＸ５０９－ＣＥＲＴ＃２を受領した端末１０は、データ処理部１１でＸ５０９－ＣＥＲＴ＃２をＥＭＶ－ＣＥＲＴ＃２に変換し（Ｔ３０４）、これをリーダライタ１４を介してＩＣカード２０に送付する。

【００５４】ＥＭＶ－ＣＥＲＴ＃２を受領したＩＣカード２０は、検証処理部２２でＥＭＶ－ＣＥＲＴ＃２の検証処理を行い（Ｉ３０１）、正当と判断できる場合は、データ格納部２３に公開鍵＃２を格納する（Ｉ３０２）。

【００５５】この結果、ＩＣカード２０はサーバ３０の公開鍵＃２を格納し、一方、サーバ３０はＩＣカード２０の公開鍵＃１を格納することになり、これらの公開鍵を用いて相互に暗号通信を行う際に、相手側のデータの検証を行えるようになる。なお、フォーマットの変換に際して、標準的なフォーマットを一つ定め、それを経由する形で個別のフォーマットへの変換ルールを定義するようにすることが好ましい。このようにすることで、個別のフォーマットの数が多くなった場合にも容易に対応できるようになる。

【００５６】

【発明の効果】以上の説明から明らかなように、本発明の公開鍵証明書によれば、複数のフォーマットを用いることが可能になるため、インフラ構築において汎用性の高いフォーマットを採用しつつＩＣカード等のリソース

16

が小さいデバイスにおいても利用可能な簡易なフォーマットを採用することが可能となるため、インフラの重複開発や、ＩＣカード等における公開鍵証明書によるリソースの浪費を防止できるようになる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係る公開鍵証明書サービスシステムの構成図。

【図２】第１実施形態による公開鍵証明書の発行手順を示した図。

【図３】Ｘ５０９公開鍵証明書とＥＭＶ公開鍵証明書との間の項目の対応図。

【図４】第１実施形態による公開鍵証明書のフォーマット変換の概念図。

【図５】本発明の第２実施形態に係る公開鍵証明書サービスシステムの認証局の構成図。

【図６】第２実施形態による公開鍵証明書の発行手順を示した図。

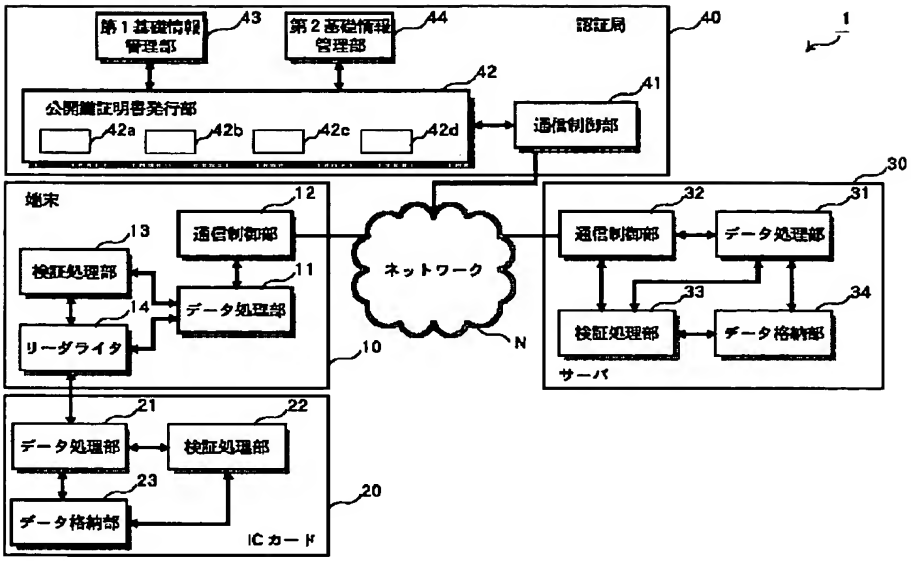
【図７】第２実施形態による公開鍵証明書のフォーマット変換の概念図。

【図８】公開鍵証明書を検証する際のＩＣカードと端末との間及び端末とサーバとの間の処理手順を示したシーケンスチャート。

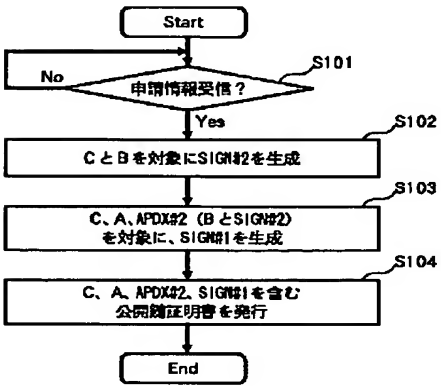
【符号の説明】

１　公開鍵証明書サービスシステム
１０　端末
１１、２１、３１　データ処理部
１２、３２、４１　通信制御部
１３、２２、３３　検証処理部
１４　リーダライタ
２０　ＩＣカード
２３、３４　データ格納部
３０　サーバ
４０　認証局
４２　公開鍵証明書発行部
４３　第１基礎情報管理部
４４　第２基礎情報管理部
Ｎネットワーク

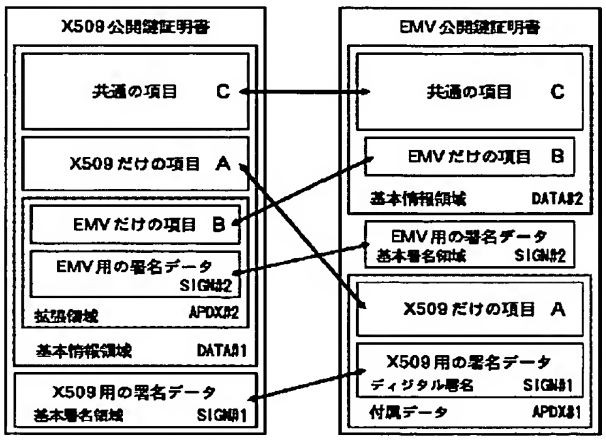
【図１】


第１基礎情報管理部
43
第２基礎情報管理部
44
認証局
40
1
公開鍵証明書発行部
42
42a
42b
42c
42d
通信制御部
41
30
端末
12
通信制御部
13
検証処理部
11
データ処理部
14
リーダライタ
10
ネットワーク
N
32
通信制御部
31
データ処理部
33
検証処理部
34
データ格納部
サーバ
21
データ処理部
22
検証処理部
23
データ格納部
20
ICカード

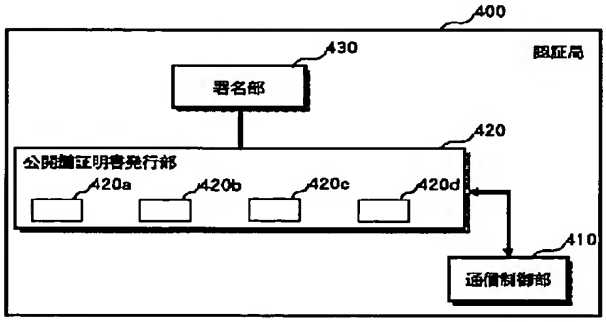
【図２】


Start
No
申請情報受信？
S101
Yes
S102
CとBを対象にSIGN#2を生成
S103
C、A、APDX#2（BとSIGN#2）を対象に、SIGN#1を生成
S104
C、A、APDX#2、SIGN#1を含む公開鍵証明書を発行
End

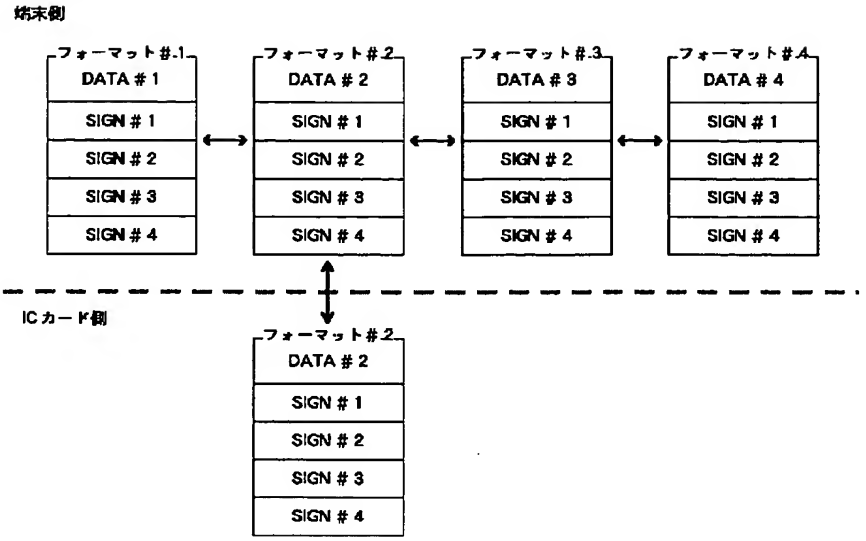
【図３】


X509公開鍵証明書
共通の項目 C
X509だけの項目 A
EMVだけの項目 B
EMV用の署名データ
SIGN#2
拡張領域
APDX#2
基本情報領域
DATA#1
X509用の署名データ
基本署名領域
SIGN#1
EMV公開鍵証明書
共通の項目 C
EMVだけの項目 B
基本情報領域
DATA#2
EMV用の署名データ
基本署名領域
SIGN#2
X509だけの項目 A
X509用の署名データ
ディジタル署名
SIGN#1
付属データ
APDX#1

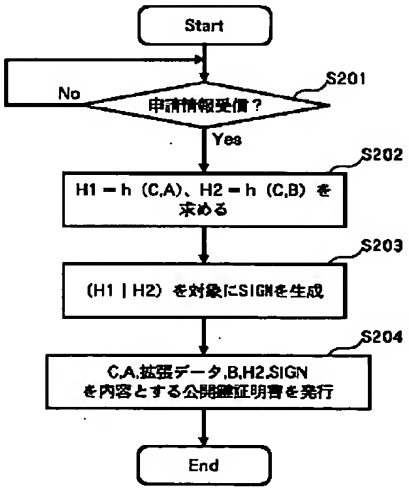
【図５】


400
認証局
430
署名部
420
公開鍵証明書発行部
420a
420b
420c
420d
410
通信制御部

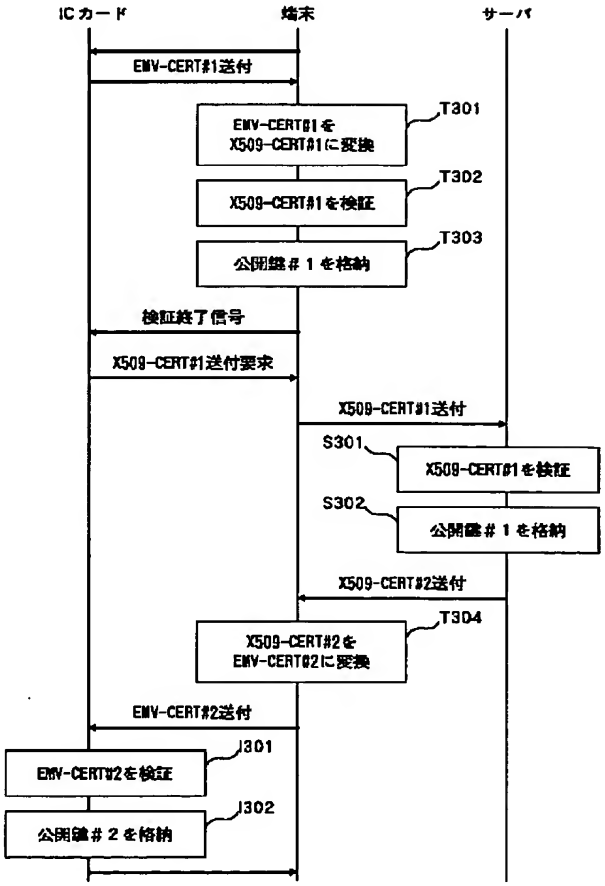
【図４】


端末側
フォーマット#.1
DATA # 1
SIGN # 1
SIGN # 2
SIGN # 3
SIGN # 4
フォーマット#.2
DATA # 2
SIGN # 1
SIGN # 2
SIGN # 3
SIGN # 4
フォーマット#.3
DATA # 3
SIGN # 1
SIGN # 2
SIGN # 3
SIGN # 4
フォーマット#.4
DATA # 4
SIGN # 1
SIGN # 2
SIGN # 3
SIGN # 4
ICカード側
フォーマット#.2
DATA # 2
SIGN # 1
SIGN # 2
SIGN # 3
SIGN # 4

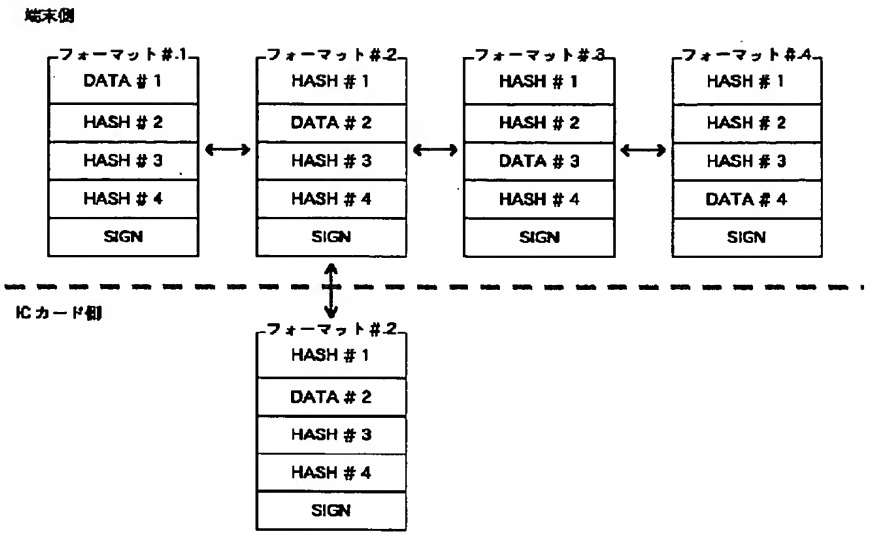
【図６】


Start
No
申請情報受信？
S201
Yes
S202
H1＝h（C,A）、H2＝h（C,B）を求める
S203
（H1｜H2）を対象にSIGNを生成
S204
C,A,拡張データ,B,H2,SIGNを内容とする公開鍵証明書を発行
End

【図８】


ICカード
端末
サーバ
EMV-CERT#1送付
T301
EMV-CERT#1をX509-CERT#1に変換
T302
X509-CERT#1を検証
T303
公開鍵＃１を格納
検証終了信号
X509-CERT#1送付要求
X509-CERT#1送付
S301
X509-CERT#1を検証
S302
公開鍵＃１を格納
X509-CERT#2送付
T304
X509-CERT#2をEMV-CERT#2に変換
EMV-CERT#2送付
301
EMV-CERT#2を検証
302
公開鍵＃２を格納

【図７】



フロントページの続き

(51) Int. Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ	